

PAT-NO: JP402199939A  
DOCUMENT-IDENTIFIER: JP 02199939 A  
TITLE: SYSTEM FOR VERIFYING OPPOSITE PARTY  
PUBN-DATE: August 8, 1990  
INVENTOR-INFORMATION:  
NAME  
SONEDAKA, NORIYOSHI  
INT-CL (IPC): H04L009/00, G09C001/00 , H04L009/10 , H04L009/12

ABSTRACT:

PURPOSE: To secure the confidentiality even when an ID number of one party is intercepted by a 3rd party and to detect the presence of a forged data by the 3rd party immediately by using both receiver and sender ID numbers.

CONSTITUTION: A basic decoding section D1 decodes a sender ID number by using a secret key S4 in common to the sender and the receiver. The secret key S4 is obtained by a selection section D1-2 selecting either a secret key S3 outputted from a secret key register section D3 or a receiver ID number S6 outputted from a receiver ID number register section D4. Then a decoded signal S5 is decoded by using the receiver ID number S4 and the decoded signal is outputted to a transmission line T1. A basic cryptographic section E1 of the receiver side ciphers the decoded signal S7 by using the receiver ID number S4. A decoded signal S8 generated from the basic cryptographic section E1 is inputted to a sender ID number verification section E2, in which a sender ID number outputted from a sender ID number register section D2 and the decoded signal S8 are compared.

COPYRIGHT: (C)1990,JPO&Japio

## ⑫ 公開特許公報(A)

平2-199939

⑤Int.Cl.<sup>5</sup>

識別記号

庁内整理番号

④公開 平成2年(1990)8月8日

H 04 L 9/00  
G 09 C 1/00  
H 04 L 9/10  
9/12

7368-5B

6945-5K H 04 L 9/00

Z

審査請求 未請求 請求項の数 1 (全6頁)

⑭発明の名称 相手認証方式

②特 願 平1-18908

②出 願 平1(1989)1月28日

⑦発 明 者 曾 根 高 則 義 東京都港区芝5丁目33番1号 日本電気株式会社内  
⑦出 願 人 日本電気株式会社 東京都港区芝5丁目7番1号  
⑦代 理 人 弁理士 芦 田 坦 外2名

## 明 細 書

## 1. 発明の名称

相手認証方式

## 2. 特許請求の範囲

1) 任意の通信路において、送信者が通信文をデジタル署名して受信者が確認する相手認証方式であって、送信者側は、 $n$ ビット( $n$ は自然数)からなる送信者ID番号ID1を受信者側と共通に取り決めた $n$ ビットからなる秘密鍵MKで復号化する所定のアルゴリズムにより $n$ ビットからなる復号化信号C1を生成する手段と、前記復号化信号C1を、 $n$ ビットからなる受信者ID番号ID2で復号化する所定のアルゴリズムにより $n$ ビットからなる復号化信号C1'を生成する手段と、該復号化信号C1'を伝送路に送出する手段とを有し、受信者側は、前記伝送路から受信した復号化信号C1'を $n$ ビットからなる受信者ID番号ID2にて暗号化する所定のアルゴリズムにより $n$

ビットからなる暗号化信号C1'を生成する手段と、前記暗号化信号C1'を、送信者側と共通に取り決めた $n$ ビットからなる秘密鍵MKで暗号化する所定のアルゴリズムにより $n$ ビットからなる送信者ID番号ID1'を生成する手段と、送信されてくる送信者ID番号ID1'と認識している送信者ID番号とが一致するかどうかを判別する手段とを有することを特徴とする相手認証方式。

## 3. 発明の詳細な説明

## 〔産業上の利用分野〕

本発明は、任意の通信路において送信者が通信文をデジタル署名して受信者が確認する相手認証方式に関する。

## 〔従来の技術〕

この種の相手認証方式については、例えば社団法人電子通信学会から昭和61年に発行された刊行物“現代暗号化理論”(217頁から239頁)にいくつかの例が示されている。

第1の例は、送信者側のID番号を送/受信者

共通の秘密鍵で復号化して送出し、受信側では秘密鍵で復号化された信号より送信者側のID番号を得る方式である。

第2の例では送信者側が送信者側のID番号を受信側に平文で送出し、その後、送信者のID番号を送／受信者共通の秘密鍵でハッシュ関数hを施し、別の秘密鍵で復号化して受信側に送出する。この第2の例では、受信側は、最初に送出されたID番号を共通秘密鍵でハッシュ関数hを施して得られる値と、後に送られてくるID番号をハッシュ関数hで圧縮して復号化した信号を別の秘密鍵で暗号化することにより得られる値とが一致するかどうか比較して相手を認証する。

第2図を参照して上記第1の方式について説明する。

まず、送信者側では、送信者ID番号レジスタ部D2より出力される送信者ID番号(IDI) S1と秘密鍵レジスタ部D3より出力される秘密鍵(MK) S4を基本復号化部D1によって復号化した後、復号化信号S5を伝送路T1に出力す

れば、

$$I D I \neq I D I' \quad \dots (2-4)$$

となる。

第3図は前述した第2の方式の構成例を示す。この方式は、送信者側で手順1として、送信者ID番号レジスタ部D2より出力される送信者ID番号(IDI) S1を伝送路T1に送出する。次に、手順2として、送信者ID番号S1を秘密鍵レジスタ部D3から出力される秘密鍵(MK) S4を使用してデータ圧縮部H1においてハッシュ関数hを施し、圧縮信号S11として基本復号化部D1に出力する。基本復号化部D1では入力した圧縮信号S11を他の秘密鍵レジスタ部D5より出力された秘密鍵(MK2) S10で復号化し、復号化信号(CI) S12として伝送路T1に出力する。

伝送路T1を経由して受信者側には送信者ID番号S1による送信者ID番号S13と復号化信号S12による復号化信号S14が供給される。

受信者側では、手順1として、受信した送信者

る。

伝送路T1を経由して受信者側には復号化信号S6が供給される。送信者側にあるものと同じ秘密鍵レジスタ部D3より出力される秘密鍵(MK) S4を用いて復号化信号S6を基本暗号化部E1によって暗号化した後、送信者ID番号認証部E2に復元信号(IDI') S8として出力する。送信者ID番号認証部E2は、期待する相手の送信者ID番号レジスタ部D2からの送信者ID番号S1と復元信号S8とを比較し、一致していれば認証結果信号S9を出力する。

この認証方式は、送信側において、

$$D(MK, IDI) = CI \quad \dots (2-1)$$

受信側において、

$$E(MK, CI) = IDI' \quad \dots (2-2)$$

期待する認証は、

$$I D I = I D I' \quad (\text{但し、} D = E^{-1}) \quad \dots (2-3)$$

ならば、相手を認証したとする方式である。

もしも、第3者において改ざん等が実施されて

ID番号(IDI') S13を送信者側にあるものと同じ秘密鍵レジスタ部D3より出力される秘密鍵(MK) S4で送信者にあるものと同じデータ圧縮部H1においてハッシュ関数hを施した後、圧縮信号(CHI') S11として送信者ID番号認証部E2に出力する。

次に、手順2として、受信した復号化信号(CI') S14に対して送信者側のものと同じ他の秘密鍵レジスタ部D5により出力される秘密鍵(MK2) S10を用いて基本暗号化部E1において暗号化を施した後、復元信号(CHI') S15として送信者ID番号認証部E2に出力する。送信者ID番号認証部E2では、圧縮信号S11と復元信号S15とを比較し、一致していれば相手認証として認証結果信号S9を出力する。

この認証方式は次式で証明できる。

送信側において、

$$\text{手順1: } H(MK, IDI) = CHI \quad \dots (3-1)$$

$$\text{手順2: } D(MK2, CHI) = CI \quad \dots (3-2)$$

受信側において、

手順1:  $H(MK, IDI') = CHI'$  ... (3-3)

手順2:  $E(MK2, CI') = CHI'$  ... (3-4)

ここで、送信者ID番号認証部E2は、  
 $CHI' = CHI'$  ... (3-5)

ならば、相手認証したとする。

もしも、第3者において改ざん等が実施されてい  
 れば、

$CHI' \neq CHI'$  ... (3-6)

となり、改ざん等の有無か期待する相手ではない  
 かの判定ができる。

[発明が解決しようとする課題]

上記第1の方式においては、2者間以上の相手  
 との通信に共通の秘密鍵を使用する場合、(2-3)  
 式が成立しても、送信側は期待した受信側と通信  
 ができるとは限らない欠点がある。

また、伝送路T1において、送信信号に伝送路  
 品質劣化の影響が存在する場合、(2-3)式が成立  
 しても相手を認証したとはならない欠点がある。

段とを有し、受信者側は、前記伝送路から受信し  
 た復号化信号Cij'をnビットからなる受信者ID  
 番号IDjにて暗号化する所定のアルゴリズム  
 によりnビットからなる暗号化信号CI'を生成  
 する手段と、前記暗号化信号CI'を、送信者側  
 と共通に取り決めたnビットからなる秘密鍵MK  
 で暗号化する所定のアルゴリズムによりnビット  
 からなる送信者ID番号IDI'を生成する手段  
 と、送信されてくる送信者ID番号IDI'と認  
 識している送信者ID番号とが一致するかどうか  
 を判別する手段とを有することを特徴とする。

本発明によれば、送信者側における復号化のアル  
 ゴリズムは、

$D(MK, IDI) = CI$  ... (1)

$D(IDj, CI) = CIj$  ... (2)

で表わされ、受信者側における暗号化のアルゴ  
 リズムは、

$E(IDj, CIj') = CI'$  ... (3)

$E(MK, CI') = IDI'$  ... (4)

で表わされる。

一方、第2の方式においては、第1の方式の欠  
 点の一部は解決されるものの、送信者ID番号が  
 平文で伝送路に送出されるため、第3者による  
 “なりすまし”が存在する可能性がある。また、  
 第1の方式と同様2者間以上の相手の通信に於い  
 て、(3-5)式が成立しても期待する受信側との交  
 信が期待できたとはならない過大なる欠点が存在  
 していた。

[課題を解決するための手段]

本発明は、任意の通信路において、送信者が通  
 信文をデジタル署名して受信者が確認する相手  
 認証方式であって、送信者側は、nビット(nは  
 自然数)からなる送信者ID番号IDIを受信者  
 側と共通に取り決めたnビットからなる秘密鍵MK  
 で復号化する所定のアルゴリズムによりnビッ  
 トからなる復号化信号CIを生成する手段と、前  
 記復号化信号CIを、nビットからなる受信者ID  
 番号IDjで復号化する所定のアルゴリズムによ  
 りnビットからなる復号化信号CIjを生成する  
 手段と、該復号化信号CIjを伝送路に送出する手

[実施例]

第1図を参照して本発明の一実施例を説明する。  
 送信者側は、手順1において次のように動作す  
 る。

基本復号化部D1によって、送信者ID番号S  
 2を送/受信共通の秘密鍵S4で復号化する。こ  
 こで、基本復号化部D1は、例えばDES(DATA  
 ENCRYPTION STANDERD)のような慣用暗号化アル  
 ゴリズムを有したものである。また、送信者ID番  
 号S2は、送信者ID番号レジスタ部D2から出  
 力された送信者ID番号S1と基本復号化部D1  
 からの出力を戻すことにより得られる復号化信号  
 S5との一方を選択する選択部D1-1により得  
 られる。手順1においては送信者ID番号S1を  
 選択したものである。更に、秘密鍵S4は、秘密  
 鍵レジスタ部D3から出力された秘密鍵S3と受  
 信者ID番号レジスタ部D4から出力された受信  
 者ID番号S6の一方を選択する選択部D1-2  
 により得られる。手順1においては秘密鍵S3を  
 選択したものである。

基本復号化部 D 1 より復号化された復号化信号 S 5 は、選択部 D 1 - 3 によって選択部 D 1 - 1 に戻る経路を選択される。

手順 2 においては次のように動作する。

基本復号化部 D 1 によって復号化信号 S 5 を受信者 I D 番号 S 4 で復号化する。第 1 の選択部 D 1 - 1 は復号化信号 S 5 を選択して S 2 とし、選択部 D 1 - 2 は受信者 I D 番号 S 6 を選択して S 4 とする。また、選択部 D 1 - 3 は手順 2 で生成された復号化信号 S 5 を選択し、伝送路 T 1 に出力する。伝送路 T 1 を通過した復号化信号は復号化信号 S 7 として受信者側に入力する。

受信者側は手順 1 において次のように動作する。

基本暗号化部 E 1 によって復号化信号 S 7 を受信者 I D 番号 S 4 で暗号化する。ここで、受信者 I D 番号 S 4 は、送信者側のものと同じ受信者 I D 番号レジスタ部 D 4 から出力された受信者 I D 番号 S 6 と送信者側のものと同じ秘密鍵レジスタ部 D 3 から出力される秘密鍵 S 3 との一方を選択する選択部 E 1 - 2 に入力され、手順 1 において

は受信者 I D 番号 S 6 を選択したものである。また、復号化信号 S 7 は、送信者側のものと同じ基本暗号化部 E 1 からの出力を戻すことにより得られる復元信号 S 8 と伝送路 T 1 を通して受信した復号化信号 S 7 との一方を選択する選択部 E 1 - 1 に入力され、手順 1 においては、復号化信号 S 7 を選択する。基本暗号化部 E 1 によって復元された復元信号 S 8 は、選択部 E 1 - 3 で選択部 E 1 - 1 に戻る経路を選択される。

手順 2 においては次のように動作する。基本暗号化部 E 1 によって、復号化信号 S 7 を秘密鍵 S 4 で暗号化する。選択部 E 1 - 1 は手順 1 で生成された復元信号 S 8 を、選択部 E 1 - 2 においては秘密鍵 S 3 を、選択部 E 1 - 3 では送信者 I D 番号認証部 E 2 に送出する経路を選択してある。

基本暗号化部 E 1 より生成された復元信号 S 8 は、送信者 I D 番号認証部 E 2 に入力される。送信者 I D 番号認証部 E 2 において、送信者 I D 番号レジスタ部 D 2 より出力された送信者 I D 番号 S 1 と復元信号 S 8 を比較し、一致しているかど

うかの結果を認証結果信号 S 9 として出力する。

1 例として、送信する信号の平文を送信者 I D 番号としたが、特に送／受信者間で任意に取り決めたデジタル署名文でもよい。

#### 〔発明の効果〕

以上説明したように、本発明の相手認証方式は、受信者と送信者の I D の両方を使用する事から、一方の I D 番号が第 3 者に分かっていても秘密は保持でき、第 3 者の改ざん等の有無も即座に検出できる。

#### 4. 図面の簡単な説明

第 1 図は、本発明の一実施例に係る相手認証方式の構成例である。

第 2 図は、従来の相手認証方式の一例を示す構成例である。

第 3 図は、従来の相手認証方式の他の構成例である。

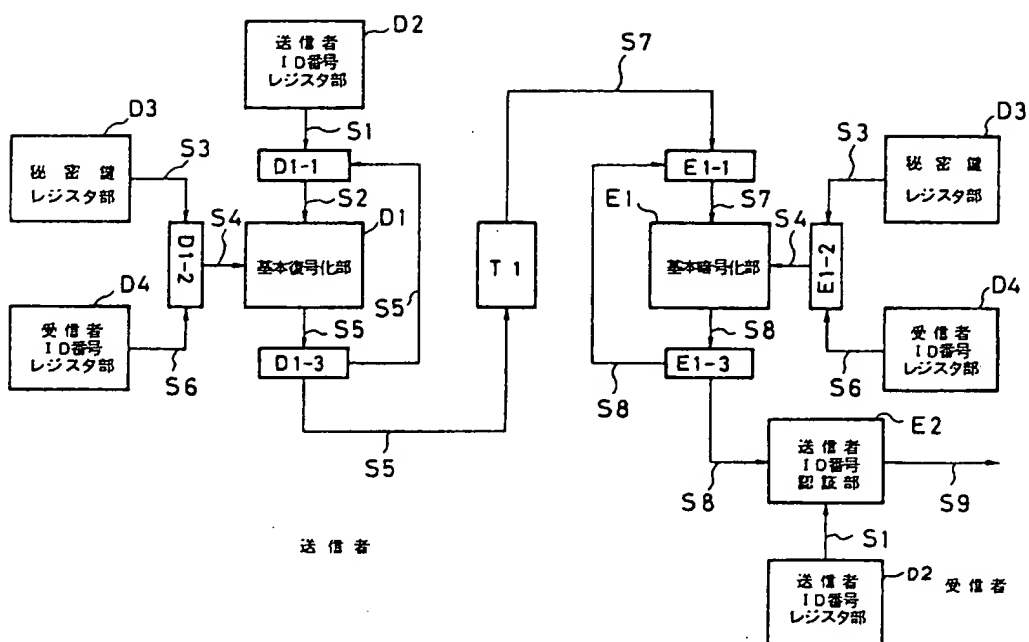
D 1 …基本復号化部、D 2 …送信者 I D 番号レジスタ部、D 3 …秘密鍵レジスタ部、D 4 …受信

者 I D 番号レジスタ部、D 5 …秘密鍵レジスタ部、E 1 …基本暗号化部、E 2 …送信者 I D 番号認証部。

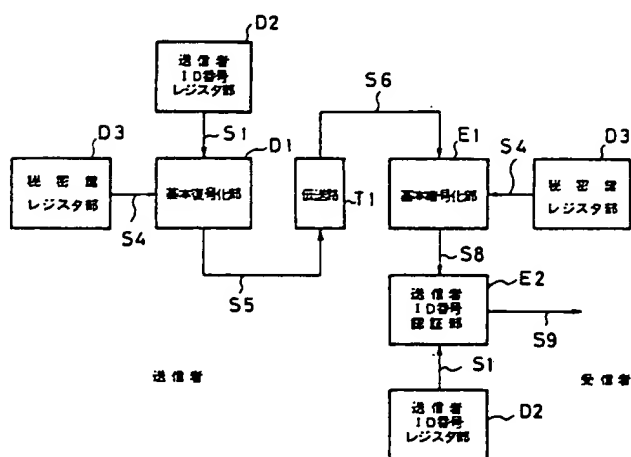
代 2 表 (7783) 発 明 者 池 田 康 保



第 1 図



第 2 圖



第 3 図

